

SYMMETRIC MODULAR DIOPHANTINE INEQUALITIES

J. C. ROSALES

(Communicated by Lance W. Small)

ABSTRACT. In this paper we study and characterize those Diophantine inequalities $ax \bmod b \leq x$ whose set of solutions is a symmetric numerical semigroup.

Given two integers a and b with $b \neq 0$ we write $a \bmod b$ to denote the remainder of the division of a by b . Following the notation used in [8], a *modular Diophantine inequality* is an expression of the form $ax \bmod b \leq x$. The set $S(a, b)$ of integer solutions of this inequality is a numerical semigroup, that is, it is a subset of \mathbb{N} (the set of nonnegative integers) closed under addition, $0 \in S(a, b)$ and such that $\mathbb{N} \setminus S(a, b)$ has finitely many elements. We say that a numerical semigroup is *modular* if it is the set of solutions to a modular Diophantine inequality. As shown in [8], not every numerical semigroup is of this form.

If S is a numerical semigroup, then the greatest integer not in S is the Frobenius number of S , denoted by $g(S)$. The numerical semigroup S is *symmetric* (see [1]) if $x \in \mathbb{Z} \setminus S$ implies $g(S) - x \in S$ (\mathbb{Z} is the set of integers). This kind of semigroup has been widely studied and characterized in the literature (see, for instance, [2, 4, 6]). We will say that the inequality $ax \bmod b \leq x$ is *symmetric* if $S(a, b)$ is a symmetric numerical semigroup.

It is well known (see, for instance, [7]) that every numerical semigroup S is finitely generated and thus there exist positive integers n_1, \dots, n_p such that

$$S = \langle n_1, \dots, n_p \rangle = \{a_1 n_1 + \dots + a_p n_p \mid a_1, \dots, a_p \in \mathbb{N}\}.$$

If no proper subset of $\{n_1, \dots, n_p\}$ generates S , then we say that this set is a minimal system of generators of S . Minimal systems of generators always exist and are unique (see [7]); the cardinality of a minimal system of generators of S is known as the *embedding dimension* of S , denoted here by $e(S)$.

Clearly, the inequality $ax \bmod b \leq x$ has the same integer solutions as the inequality $(a \bmod b)x \bmod b \leq x$. Thus we may assume (and in fact we will) that $a, b \in \mathbb{N}$ and $a < b$. Note that $S(0, b) = \mathbb{N}$ is trivially symmetric.

Throughout this paper (and unless otherwise stated) we will assume that a and b are positive integers, and that $d = \gcd\{a, b\}$ and $d' = \gcd\{a-1, b\}$ (\gcd stands for greatest common divisor). In Proposition 4, we will show that $S(a, b)$ is symmetric if and only if $S(a, b) = \langle b/d, b/d', d+d' \rangle$. Theorem 5 characterizes those pairs (a, b)

Received by the editors April 8, 2004 and, in revised form, June 21, 2005.

2000 *Mathematics Subject Classification*. Primary 20M14.

The author was supported by the project BFM2000-1469 and thanks P. A. García-Sánchez for his comments and suggestions.

such that $S(a, b)$ is symmetric. As a consequence, in Corollary 6 we show that S is a modular symmetric numerical semigroup if and only if $S = \langle kt, kt', t + t' \rangle$ where k, t, t' are positive integers such that $\gcd\{t, t'\} = \gcd\{k, t + t'\} = 1$. If S is a numerical semigroup with $e(S) \leq 2$, then by [5], S is symmetric and by [9] we know that S is modular. Proposition 9 states that $e(\langle kt, kt', t + t' \rangle) = 3$ if and only if $1 \notin \{t, t', k\}$. We finish the paper proposing the open question of deciding for which positive integers g there exists a modular symmetric numerical semigroup with embedding dimension three and Frobenius number g .

The following result is a consequence of Corollaries 6, 16 and 17, and Lemma 11 in [8]. Recall that a and b are positive integers, with $a < b$ and that $d = \gcd\{a, b\}$ and $d' = \gcd\{a - 1, b\}$.

Lemma 1. 1) If $x \in \mathbb{Z} \setminus S(a, b)$, then $b - x \in S(a, b)$.

2) Let x be a positive integer. Then $x \in S(a, b)$ and $b - x \in S(a, b)$ if and only if

$$x \in \left\{k \frac{b}{d} \mid 0 \leq k \leq d - 1\right\} \cup \left\{k \frac{b}{d'} \mid 0 \leq k \leq d' - 1\right\}.$$

3) $b - d - d' \geq g(S(a, b))$.

4) $S(a, b)$ is symmetric if and only if $g(S(a, b)) = b - d - d'$.

The next result is broadly used throughout this paper.

Lemma 2. $S(a, b)$ is symmetric if and only if $b - d - d' \notin S(a, b)$.

Proof. If $S(a, b)$ is symmetric, then by 4) in Lemma 1, we know that $g(S(a, b)) = b - d - d'$ and thus $b - d - d' \notin S(a, b)$. Conversely, if $b - d - d' \notin S(a, b)$, then by 3) in Lemma 1, we deduce that $g(S(a, b)) = b - d - d'$, which in view of 4) in Lemma 1 implies that $S(a, b)$ is symmetric. \square

In order to prove Proposition 4, we need the following result which can be deduced from [5].

Lemma 3. If $S = \langle n_1, n_2, n_3 \rangle$ is a numerical semigroup and $(\gcd\{n_1, n_2\})n_3 \in \langle n_1, n_2 \rangle$, then S is symmetric.

Proposition 4. $S(a, b)$ is symmetric if and only if $S(a, b) = \langle \frac{b}{d}, \frac{b}{d'}, d + d' \rangle$.

Proof. If $S(a, b)$ is symmetric, then by Lemma 2 we know that $b - d - d' \notin S$. Hence by 1) in Lemma 1, $d + d' \in S(a, b)$. Besides, $a \frac{b}{d} \bmod b = 0$ and $a \frac{b}{d'} \bmod b = ((a - 1) \frac{b}{d'} + \frac{b}{d'}) \bmod b = \frac{b}{d'} \bmod b \leq \frac{b}{d'}$. Hence $\{\frac{b}{d}, \frac{b}{d'}, d + d'\} \subseteq S(a, b)$. Consequently, $\langle \frac{b}{d}, \frac{b}{d'}, d + d' \rangle \subseteq S(a, b)$. For the other inclusion, take $x \in S(a, b)$ and let $t = \max\{k \in \mathbb{N} \mid x - k(d + d') \in S(a, b)\}$. Then $x - (t + 1)(d + d') \notin S(a, b)$. By using that $S(a, b)$ is symmetric and that $g(S(a, b)) = b - d - d'$, we obtain that $b - d - d' - x + (t + 1)(d + d') = b - (x - t(d + d')) \in S(a, b)$. As $x - t(d + d')$ is also in $S(a, b)$, by 2) in Lemma 1 we conclude that $x \in \langle \frac{b}{d}, \frac{b}{d'}, d + d' \rangle$.

Conversely, since $\gcd\{a, a - 1\} = 1$, then $\gcd\{d, d'\} = 1$ and thus $\gcd\{\frac{b}{d}, \frac{b}{d'}\} = \frac{b}{dd'}$. As $\frac{b}{dd'}(d + d') = \frac{b}{d'} + \frac{b}{d} \in \langle \frac{b}{d}, \frac{b}{d'} \rangle$, by Lemma 3, we conclude that $S(a, b)$ is symmetric. \square

Note that as an immediate consequence of this proposition, we have that if $S(a, b)$ is symmetric, then $e(S(a, b)) \leq 3$. In view of [5], we deduce that if S is a modular numerical semigroup, then S is symmetric if and only if S is a complete intersection; or equivalently, S is free in the sense of [3].

Given two integers x and y , denote by $x \mid y$ the fact that x divides y .

Theorem 5. $S(a, b)$ is symmetric if and only if $(a, b) = (ut, ktt')$ for some positive integers t, t', u, v and k such that $ut - vt' = 1$ and $k|u + v$.

Proof. Necessity. Since $d = \gcd\{a, b\}$ and $d' = \gcd\{a - 1, b\}$, there exist positive integers u, v and k such that $a = ud, a - 1 = vd'$ and $b = kdd'$. Note that $ud - vd' = 1$ and $(a, b) = (ud, kdd')$. We show that if $S(a, b)$ is symmetric, then $k | u + v$. If $k = 1$, this assertion trivially holds. Thus, in the following we will assume that $k \geq 2$. We distinguish two cases depending on the value of d' .

- 1) Assume that $d' = 1$. If $(1 + u + v) \bmod k = 0$, then $(ud)(d + 1) \bmod kd = 0$, since $(ud)(d + 1) \bmod kd = (d(1 + v) + ud) \bmod kd = d((1 + u + v) \bmod k) = 0$. Hence $ud(kd - (d + 1)) \bmod kd = 0$ and thus $kd - d - 1 \in S(ud, kd)$. But this is impossible, since $(ud, kd) = (a, b)$ and as $S(a, b)$ is symmetric, by Lemma 2, $kd - d - 1 = b - d - d' \notin S(ud, kd) = S(a, b)$. Therefore, $(1 + u + v) \bmod k \neq 0$. By using the equalities seen above, $ud(kd - d - 1) \bmod kd = kd - d((1 + u + v) \bmod k)$. As $kd - d - 1 \notin S(ud, kd)$, we deduce that $kd - d((1 + u + v) \bmod k) > kd - d - 1$, whence $d + 1 > d((1 + u + v) \bmod k)$. This implies that $(1 + u + v) \bmod k = 1$ and this leads to $(u + v) \bmod k = 0$. This proves that $k | u + v$.
- 2) Assume now that $d' \geq 2$. Note that

$$\begin{aligned} ud(d + d') \bmod kdd' &= (d(1 + vd') + udd') \bmod kdd' \\ &= (d + (u + v)dd') \bmod kdd' \\ &= (d + dd'((u + v) \bmod k)) \bmod kdd' \\ &= d + dd'((u + v) \bmod k). \end{aligned}$$

The last equality holds because $d' \geq 2$ and thus $d + dd'((u + v) \bmod k) \leq d + dd'(k - 1) < kdd'$. Hence

$$ud(kdd' - d - d') \bmod kdd' = kdd' - d - dd'((u + v) \bmod k).$$

As $S(ud, kdd') = S(a, b)$ is symmetric, by Lemma 2, we have that $kdd' - d - d' \notin S(ud, kdd')$ and consequently

$$kdd' - d - dd'((u + v) \bmod k) = ud(kdd' - d - d') \bmod kdd' > kdd' - d - d'.$$

This implies that $d' > dd'((u + v) \bmod k)$ and this forces $(u + v) \bmod k = 0$. This proves that $k | u + v$ holds.

Sufficiency. Clearly, $\gcd\{ut, (u + v)tt'\} = t$ and $\gcd\{ut - 1, (u + v)tt'\} = \gcd\{vt', (u + v)tt'\} = t'$. By using that k divides $u + v$, we obtain that $\gcd\{ut, ktt'\} = t$ and $\gcd\{ut - 1, ktt'\} = t'$. We apply Lemma 2 to prove that $S(ut, ktt')$ is symmetric. It suffices to show that $ktt' - t - t' \notin S(ut, ktt')$. Note that for $k = t' = 1$, the result follows trivially, since $S(ut, t) = S(0, t) = \mathbb{N}$, which is symmetric. Thus, assume that $k \geq 2$ or $t' \geq 2$. Note that $ut(t + t') \bmod ktt' = (t(1 + vt') + utt') \bmod ktt' = (t + (u + v)tt') \bmod ktt' = t$, since $k | u + v$ and $t < ktt'$ because $k \geq 2$ or $t' \geq 2$. Hence $ut(ktt' - t - t') \bmod ktt' = ktt' - t > ktt' - t - t'$. This implies that $ktt' - t - t' \notin S(ut, ktt')$ and this concludes the proof. \square

Corollary 6. Let S be a numerical semigroup. Then S is symmetric and modular if and only if $S = \langle kt, kt', t + t' \rangle$, where t, t' and k are positive integers such that $\gcd\{t, t'\} = \gcd\{k, t + t'\} = 1$. Moreover, if this holds, then $g(S) = ktt' - t - t'$.

Proof. If S is a modular numerical semigroup, then there exist positive integers a and b such that $S = S(a, b)$. If, in addition, S is symmetric, then by Proposition 4 we

have that $S = S(a, b) = \langle \frac{b}{d}, \frac{b}{d'}, d + d' \rangle$, where $d = \gcd\{a, b\}$ and $d' = \gcd\{a - 1, b\}$. Note that $\gcd\{d, d'\} = 1$ and if $k = \frac{b}{dd'}$, then $S = \langle kd, kd', d + d' \rangle$. As S is a numerical semigroup $\gcd\{kd, kd', d + d'\} = 1$, whence $\gcd\{k, d + d'\} = 1$.

Conversely, as $\gcd\{t, t'\} = \gcd\{k, t + t'\} = 1$, we have that $\gcd\{kt, t + t'\} = 1$. Thus there exist positive integers u, v such that $ukt - v(t + t') = 1$, or equivalently $(uk - v)t - vt' = 1$. Besides, k trivially divides $uk - v + v$. We can apply Theorem 5 and deduce that $S((uk - v)t, ktt')$ is symmetric. Then in view of Proposition 4, we know that $S((uk - v)t, ktt') = \langle kt, kt', t + t' \rangle$ and by Lemma 2, $g(S) = ktt' - t - t'$. \square

Example 7. If we use Corollary 6 with $t = 2, t' = 3$ and $k = 7$, then $S := \langle 14, 21, 5 \rangle$ is a modular symmetric numerical semigroup with $g(S) = 37$. Moreover, from the proof of the above mentioned corollary, we can obtain a couple of positive integers a, b such that $S = S(a, b)$. It suffices to observe that $kt = 14, t + t' = 5$ and $4 \times 14 - 11 \times 5 = 1$. Hence $u = 4$ and $v = 11$, which implies that $S = S((uk - v)t, ktt') = S(34, 42) = \langle 14, 21, 5 \rangle$.

Example 8. $S := \langle 6, 7, 9 \rangle = \{0, 6, 7, 9, 12, 13, 14, 15, 16, 18, \rightarrow\}$ (the arrow means that from this point on, every integer belongs to the set) is a symmetric numerical semigroup with $g(S) = 17$. By using Corollary 6, we can deduce that S is not modular, since there are no positive integers k, t and t' such that $\gcd\{t, t'\} = \gcd\{k, t + t'\} = 1$ and $\{6, 7, 9\} = \{kt, kt', t + t'\}$.

Proposition 9. Let k, t and t' be positive integers such that

$$\gcd\{t, t'\} = \gcd\{k, t + t'\} = 1.$$

Then $e(\langle kt, kt', t + t' \rangle) = 3$ if and only if $1 \notin \{k, t, t'\}$.

Proof. If $t = 1$, then $\langle k, kt', t + t' \rangle = \langle k, 1 + t' \rangle$. Thus $e(\langle kt, kt', t + t' \rangle) \leq 2$. The cases $t' = 1$ and $k = 1$ are analogous.

Conversely, as $k \neq 1$, we have that $t + t' \notin \langle kt, kt' \rangle$, since otherwise k would divide $t + t'$, in contradiction with $\gcd\{k, t + t'\} = 1$. If $kt \in \langle kt', t + t' \rangle$, then $kt = rkt' + s(t + t')$ for some nonnegative integers r and s . The fact that $\gcd\{k, t + t'\} = 1$, implies that k divides s and thus we can write $t = rt' + \frac{s}{k}(t + t')$. But this forces $s/k = 0$ and $t = rt'$, because $t, t' > 1$, contradicting that $\gcd\{t, t'\} = 1$. Analogously, one proves that $kt' \notin \langle kt, t + t' \rangle$. This shows that $e(\langle kt, kt', t + t' \rangle) = 3$. \square

It is well known (and easy to prove) that the Frobenius number of a symmetric numerical semigroup is always an odd integer. If g is an odd positive integer, then in view of Corollary 6 with $t = t' = 1$ and $k = g + 2$, we deduce that $\langle 2, g + 2 \rangle$ is a symmetric modular numerical semigroup with Frobenius number g (this actually was already known to us prior to Corollary 6, since $\langle 2, g + 2 \rangle$ is symmetric with Frobenius number g and it is modular in view of [9]). As we will see in Example 11, there is no symmetric modular numerical semigroup with embedding dimension three and Frobenius number nine. So the natural question arises: For which values of g there exists a symmetric modular numerical semigroup with embedding dimension three and Frobenius number g ? As a consequence of Corollary 6 and Proposition 9 we obtain the following result, which answers (though not in an effective way) the above question.

Corollary 10. Let g be a positive integer. Then there exists a symmetric modular numerical semigroup with embedding dimension three and Frobenius number g if

and only if $g = ktt' - t - t'$ for some integers greater than or equal to two such that $\gcd\{t, t'\} = \gcd\{k, t + t'\} = 1$.

Example 11. We prove that there are no symmetric modular numerical semigroups with embedding dimension three and Frobenius number nine. By using Corollary 10, it suffices to show that nine cannot be expressed as $ktt' - t - t'$ with $k, t, t' \geq 2$ and $\gcd\{t, t'\} = \gcd\{k, t + t'\} = 1$. As $tt' \geq t + t'$, if $9 = ktt' - t - t'$, then $(k - 1)tt' \leq 9$. From the conditions imposed on k, t and t' , we deduce that $k = 2$ and $\{t, t'\} = \{2, 3\}$. But then $ktt' - t - t' = 7 \neq 9$.

We finish this work with an example where we give some families of positive integers g for which there exists a symmetric modular numerical semigroup of embedding dimension three and Frobenius number g .

Example 12.

- If we apply Corollary 10 to $t = 2$ and $t' = 3$, then we obtain that there exist symmetric modular numerical semigroups with embedding dimension three and Frobenius number g , for every g in the set

$$\{k6 - 5 \mid k \geq 2, \gcd\{k, 5\} = 1\} = \{7, 13, 19, 31, \dots\}.$$

- For $t = 2$ and $t' = 5$ we obtain the set

$$\{k10 - 7 \mid k \geq 2, \gcd\{k, 7\} = 1\} = \{13, 23, 33, 43, 53, 73, \dots\}.$$

- For $t = 3$ and $t' = 4$ one gets the set

$$\{k12 - 7 \mid k \geq 2, \gcd\{k, 7\} = 1\} = \{17, 29, 41, 53, 65, 89, \dots\}.$$

REFERENCES

- [1] R. Apéry, Sur les branches superlinéaires des courbes algébriques, C. R. Acad. Sci. Paris, **222** (1946). MR0017942 (8:221a)
- [2] V. Barucci, D. E. Dobbs and M. Fontana, “Maximality properties in numerical semigroups and applications to one-dimensional analytically irreducible local domains”, *Memoirs of the Amer. Math. Soc.* **598** (1997). MR1357822 (97g:13039)
- [3] J. Bertin and P. Carbone, Semi-groupes d’entiers et application aux branches, *J. Algebra* **49** (1987), 81-95. MR0568894 (58:27957)
- [4] R. Fröberg, G. Gottlieb and R. Häggkvist, On numerical semigroups, *Semigroup Forum* **35** (1987), 63-83. MR0880351 (88d:20092)
- [5] J. Herzog, Generators and relations of abelian semigroups and semigroup rings, *Manuscripta Math.*, **3** (1970), 175-193. MR0269762 (42:4657)
- [6] E. Kunz, The value-semigroup of a one-dimensional Gorenstein ring, *Proc. Amer. Math. Soc.*, **25** (1973), 748-751. MR0265353 (42:263)
- [7] J. C. Rosales and P. A. García-Sánchez, “Finitely generated commutative monoids,” Nova Science Publishers, New York, 1999. MR1694173 (2000d:20074)
- [8] J. C. Rosales, P. A. García-Sánchez and J. M. Urbano-Blanco, Modular Diophantine inequalities and numerical semigroups, *Pacific J. Math.* **218** (2005), 379-398.
- [9] J. C. Rosales, P. A. García-Sánchez, J. I. García-García and J. M. Urbano-Blanco, Proportionally modular Diophantine inequalities, *J. Number Theory* **103** (2003), 281-294. MR2020273 (2004k:20127)

DEPARTAMENTO DE ÁLGEBRA, UNIVERSIDAD DE GRANADA, E-18071 GRANADA, SPAIN
E-mail address: jrosales@ugr.es